PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)
	)
Barton et al.	) Art Unit: 2137
	)
Application No. 09/916,929	) Examiner: Pyzocha, Michael J.
	)
Filed: 07/26/2001	) Atty. Docket No.:
	) NAI1P014/01.128.01
For: ANTI-VIRUS SCANNING CO-PROCESSOR	)
	) Date: 06/26/2007
	)
	)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

REPLY BRIEF (37 C.F.R. § 41.37)

This Reply Brief is being filed within two (2) months of the mailing of the Examiner's Answer mailed on 04/27/2007.

Following is an issue-by-issue reply to the Examiner's Answer.

Issue #1:

The rejection of Claims 2, 18, and 34-37 under 35 U.S.C. 112, second paragraph has been withdrawn by the Examiner.

Issue #2:

The Examiner has rejected Claims 1-2, 4-13, 17-18, 20-29, 33-35, 38-40, 42 and 44 under 35 U.S.C. 102(e) as being anticipated by Grupe et al. (U.S. Publication No. 2002/0194212).

Group #1: Claims 1, 4-7, 9-11, 13, 17, 20-23, 25-27, 29, 33, 40, and 42

The Examiner has relied on Paragraphs 0008, and 0009 from Grupe to meet appellant's claimed technique "wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit" (see this or similar, but not necessarily identical language in the independent Claims 1, 17, and 33).

> "Viewed from one aspect the present invention provides a computer program product comprising **a computer program operable to control a scanning computer to produce a log file identifying computer data from a source computer having specified content,** said computer program comprising: scanning logic operable to scan computer data transferred from said source computer to said scanning computer and to identify one or more portions of said computer data having one or more predetermined characteristics indicative of said computer data having said specified content; and log generating logic operable to write details of said identified portions to a log file.
>
> The invention recognises the above problem of scans of computer data that take so long that a complete scan of the data cannot be performed during slack time, such as overnight or during the weekend. **To address this problem embodiments of the invention transfer data to be scanned from a source computer to a scanning computer. The scanning computer then scans the data and creates a log file identifying portions of the data that have predetermined characteristics indicating a particular specified content.** This enables the source computer to rescan or otherwise selectively process the data identified in the log file, which considerably reduces the processing time of the source computer needed for a scan." (Paragraphs 0008-0009 - emphasis added)

Appellant respectfully asserts that the excerpts from Grupe relied upon by the Examiner merely disclose "a computer program operable to control a scanning computer to produce a log file

identifying computer data from a source computer having specified content." Further, Grupe discloses that "data to be scanned [is transferred] from a source computer to a scanning computer" where "[t]he scanning computer then scans the data and creates a log file identifying portions of the data that have predetermined characteristics indicating a particular specified content" (emphasis added). However, the mere disclosure of transferring data from a source computer to a scanning computer, where the scanning computer scans the data and creates a log file, as in Grupe, fails to even suggest a technique "wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit" (emphasis added), as claimed by appellant. Clearly, since the scanning computer disclosed by Grupe is not under the control of the source computer, then Grupe fails to disclose "wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 04/27/2007, the Examiner has argued that "[t]he sending of data from the source computer (i.e. the central processing unit) to the scanning computer (i.e. the co-processor) is an instruction to scan the data sent because the scanning computer scans the data as the next step after receiving the data." The Examiner has further stated that "[s]ince the scanning computer is instructed by the source computer to scan the data from [the] source computer it is under the control of the source computer."

Appellant respectfully disagrees and notes that Grupe merely discloses a "transfer [of] data to be scanned from a source computer to a scanning computer" and that the "[t]he scanning computer then scans the data" (emphasis added). However, merely transferring data from a source computer to a scanning computer, where it is then scanned, as in Grupe, does not teach a technique "wherein the scanning co-processor is under the control of the central processing unit via the execution of the scanning control logic by the central processing unit"(emphasis added), as claimed by appellant.

Furthermore, the Examiner has relied on Paragraph 0009 from Grupe to make a prior art showing of appellant's claimed technique "wherein additional data to be scanned by the scanning co-processor is queued while waiting for the results from the scanning co-processor" (see this or similar, but not necessarily identical language in the independent Claims 1, 17, and 33).

> "The invention recognises the above problem of scans of computer data that take so long that a complete scan of the data cannot be performed during slack time, such as overnight or during the weekend. To address **this problem embodiments of the invention transfer data to be scanned from a source computer to a scanning computer. The scanning computer then scans the data and creates a log file identifying portions of the data that have predetermined characteristics indicating a particular specified content.** This enables the source computer to rescan or otherwise selectively process the data identified in the log file, which considerably reduces the processing time of the source computer needed for a scan." (Paragraph 0009 - emphasis added)

Appellant respectfully asserts that the excerpt from Grupe relied upon by the Examiner merely discloses that "data to be scanned [is transferred] from a source computer to a scanning computer" where "[t]he scanning computer **then** scans the data and creates a log file identifying portions of the data that have predetermined characteristics indicating a particular specified content" (emphasis added). However, the mere disclosure that the data to be scanned is transferred to the scanning computer where the scanning computer then scans the data and creates a log file, as in Grupe, fails to even suggest a technique "wherein additional data to be scanned by the scanning co-processor is queued **while** waiting for the results from the scanning co-processor" (emphasis added), as claimed by appellant. Clearly, transferring the data to be scanned and then scanning the data, as in Grupe, fails to suggest "[queuing] additional data to be scanned... **while** waiting for the results from the scanning co-processor" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 04/27/2007, the Examiner has further relied on Paragraph 0034 of Grupe and has argued that "Grupe discloses the files are sent and scanned by the scanning computer and once all the files have been scanned the log is sent to the source computer." The Examiner has further stated that "[t]herefore, the files that have yet to be scanned are stored while waiting for the results because the results are not sent until all of the data has been scanned."

Appellant respectfully disagrees with the Examiner's allegations, and asserts that the excerpt from Grupe relied on by the Examiner merely teaches that "all of the files from [a] volume... of the main computer are copied to a scanning computer" and that "[t]he scanning computer **then** scans the copied files" (Paragraph 0034 – emphasis added). Further, Grupe discloses that "[w]hen all the copied files have been scanned the log file is sent back to the main computer" (Paragraph 0034 – emphasis added). However, merely copying all files to a scanning computer, scanning all copied files, and sending a log back to a main computer after all files have been scanned, as in Grupe, does

not teach a technique "wherein additional data to be scanned by the scanning co-processor is queued while waiting for the results from the scanning co-processor" (emphasis added), as claimed by appellant. Clearly, copying the files to a scanning computer, and then scanning the copied files, as in Grupe, simply fails to even suggest that "additional data to be scanned... is queued while waiting for the results" (emphasis added), in the manner as claimed by appellant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Grupe reference, especially in view of the arguments made hereinabove.

Group #2: Claims 2 and 18

The Examiner has relied on Paragraph 0015 from Grupe to make a prior art showing of appellant's claimed "processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is not detected."

> "A further aspect of the present invention provides a computer program product comprising a computer program operable to control a source computer to scan computer data stored by said source computer to identify one or more portions of said computer data having one or more predetermined characteristics indicative of said computer data having some specified content, said computer program comprising: **log reading logic operable to control said source computer to read a log file written by a scanning computer, said log file identifying portions of said computer data having said predetermined characteristics; and response logic responsive to said log file and operable to control said source computer to perform further processing tasks upon at least said data identified in said log file as having said predetermined characteristics.**" (Paragraph 0015 - emphasis added)

Appellant respectfully asserts that the excerpt from Grupe relied upon by the Examiner merely discloses that "log reading logic [is] operable to control said source computer to read a log file

written by a scanning computer [where] said log file identif[ies] portions of said computer data having said predetermined characteristics" (emphasis added). Further, Grupe discloses that "said source computer ... perform[s] further processing tasks upon at least said data identified in said log file as having said predetermined characteristics" (emphasis added). However, the mere disclosure of performing further processing tasks upon a log file which identifies portions of computer data having predetermined characteristics, as in Grupe, fails to even suggest "processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is **not** detected" (emphasis added), as claimed by appellant.

In the Office Action mailed 05/01/2006, the Examiner argued that "the log file allows the user to ascertain which data is malicious (needing re-scanning)" and "[t]he other data is clean." Appellant respectfully disagrees and asserts that Grupe merely discloses that "said log file identif[ies] portions of said computer data having said predetermined characteristics" (emphasis added). Clearly, identifying portions of computer data having predetermined characteristics, as in Grupe, fails to even suggest "the receipt of favorable results from the scanning co-processor including a situation where malicious code is **not** detected" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 04/27/2007, the Examiner has further relied on Paragraph 0030 of Grupe, and has asserted that "[w]hen the live system receives the log file containing a list of infected files, any file that is not on the list has favorable results." The Examiner has further stated that "[t]herefore when the files copied from the live system to the backup system are the complete set of files stored on the computer (see paragraph [0031]), the files not in the log file would be utilized as normal by the live system."

Appellant respectfully disagrees and notes that the above excerpts from Grupe relied on by the Examiner merely teach that "a copy of the live data on a "live" system... is sent... to a backup system" (Paragraph 0030). The excerpts further teach that "[t]he backup system then scans... the copied data for predetermined characteristics... creates a log file and writes... details of such data to the log file... [and] sends... the log file back to the live system" (Paragraph 0030). Further, the excerpts teach that "[t]he live system then scans any live data that is indicated in the log file"

(Paragraph [0030] – emphasis added), where "said log file identif[ies] portions of said computer data having said predetermined characteristics" (Paragraph 0015 – emphasis added).

However, appellant points out that simply nowhere in the above excerpts from Grupe relied on by the Examiner is it taught that "any file that is not on the list has favorable results," as alleged by the Examiner. The above excerpts teach that "said log file identif[ies] portions of said computer data having said predetermined characteristics," and therefore, any portions of computer data not on the list simply do not have the predetermined characteristics that the backup system scanned for.

Further, merely scanning copied data for predetermined characteristics, creating and sending a log file, and scanning data indicated in the log file that has the predetermined characteristics, as in Grupe, simply fails to even suggest "the receipt of favorable results from the scanning co-processor," much less "processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is not detected" (emphasis added), as claimed by appellant. Clearly, a log file containing details of data with predetermined characteristics, as in Grupe, simply fails to suggest "the receipt of favorable results from the scanning co-processor including a situation where malicious code is not detected" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that appellant's specific claim language is not anticipated by the Grupe reference since all of appellant's claim limitations have not been met by the Grupe reference, as noted above.

Group #3: Claims 8 and 24

The Examiner has relied on Paragraphs 0010 and 0011 in Grupe to make a prior art showing of appellant's claimed technique "wherein the event is initiated under the control of the scanning control logic."

> "Although the log file may be transferred back to the source computer by the use of tapes or disks, **it is preferable that the computer program product comprises log transferring logic operable to control said scanning computer to transfer said log file, via a network connection to said source computer.**

> Although any content of data that the user cares to specify may be scanned for, embodiments of the invention are particularly well suited to scanning for one or more of: a computer virus; a worm; a Trojan; and a computer file comprising banned content. Alternatively, embodiments of the invention can be used as part of an e-mail or file storage filtering system, wherein the specified content includes banned words or phrases." (Paragraphs 0010-0011 - emphasis added)

Appellant respectfully asserts that "log transferring logic [is] operable to control said scanning computer to transfer said log file, via a network connection to said source computer" (emphasis added). However, the mere disclosure that log transferring logic transfers the log file from the scanning computer to the source computer fails to even suggest a technique "wherein the event is initiated under the control of the scanning control logic" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 04/27/2007, the Examiner has further relied upon Paragraphs 0015-0016 in Grupe and asserts that 'Grupe discloses a computer program product comprising "a computer program operable to control a source computer to scan computer data" (paragraph [0015]) and "a computer program operable to control said source computer to transmit at least one further fraction of said data to at least one further scanning computer" (paragraph [0016]).' Further, the Examiner has argued that "[t]herefore, Grupe discloses initiating an event (the scanning of data) either by scanning the data itself (paragraph [0015]) or sending it to a scanning computer (paragraph [0016]) using scanning control logic (the computer program)."

Appellant respectfully disagrees and notes that, as admitted by the Examiner, the event initiated in Grupe is "the scanning of data" (emphasis added). However, initiating the scanning of data does not teach, and in fact *teaches away* from, a technique "wherein the event is initiated under the control of the scanning control logic" (emphasis added), where the "event [is initiated] based on the **results** from the **scanning** co-processor" (emphasis added), as claimed by appellant.

As a result, "control[ling] a source computer to scan computer data stored by said source computer" (Paragraph 0015 – emphasis added) and "control[ling] said source computer to transmit at least one further fraction of said data to at least one further scanning computer" (Paragraph 0016 – emphasis added) do not teach, and in fact *teaches away* from, a technique "wherein the event is initiated under the control of the scanning control logic" (emphasis added), where the "event [is initiated] based on the results from the scanning co-processor" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that appellant's specific claim language is not anticipated by the Grupe reference since all of appellant's claim limitations have not been met by the Grupe reference, as noted above.

Group #4: Claims 12 and 28

The Examiner has relied on Paragraphs 0011 and 0028 in Grupe to make a prior art showing of appellant's claimed technique "wherein virus signatures are stored in the memory."

> "Although any content of data that the user cares to specify may be scanned for, embodiments of the invention are particularly well suited to scanning for one or more of: a computer virus; a worm; a Trojan; and a computer file comprising banned content. Alternatively, embodiments of the invention can be used as part of an e-mail or file storage filtering system, wherein the specified content includes banned words or phrases." (Paragraph 0011)

> "In operation the network storage device 18 is subject to regular on-demand scans to identify computer viruses, Trojans, Worms and/or files with banned content. **As the network storage device 18 can be very large, the amount of processing time required to compare every stored file against an increasing number of virus definition profiles can be extremely long.** In general, the server 4 performs such scans during quiet times, such as the night or weekend. Given the increasing length of time required for such scans, it may well be that it is not possible to complete these scans during the quiet times. This could result in incomplete scans which carry the risk of viruses going undetected. " (Paragraph 0028 - emphasis added)

Appellant respectfully asserts that the excerpts from Grupe relied upon by the Examiner merely disclose that "[a]s the network storage device 18 can be very large, the amount of processing time required to compare every **stored file** against an increasing number of virus definition profiles can be extremely long" (emphasis added). However, the mere disclosure in Grupe that the stored files are compared against an increasing number of virus definition profiles fails to teach a technique "wherein virus signatures are stored in the memory" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 04/27/2007, the Examiner has argued that "in order to make any type of comparison in a processor each value involved in this comparison must be stored in some type of memory because if both values were not stored, one value would not be available for

comparison." The Examiner has further argued that "[t]herefore, when comparing the files against virus definition profiles, both the file and the definition profiles must be held in memory."

Appellant respectfully disagrees and points out that merely alleging that it is necessary to store files and virus definition profiles in some type of memory in order to compare them fails to teach a technique "wherein virus signatures are stored in the memory" (emphasis added), where the memory is included in "the scanning co-processor" (emphasis added), in the context as claimed by appellant. Thus, appellant again notes that the above excerpts relied on by the Examiner fail to teach a technique "wherein virus signatures are stored in the memory" (emphasis added), as claimed by appellant. It thus appears that the Examiner has simply not considered the full weight of appellant's claims.

Again, appellant respectfully asserts that appellant's specific claim language is not anticipated by the Grupe reference since all of appellant's claim limitations have not been met by the Grupe reference, as noted above.

Group #5: Claims 34 and 35

Furthermore, the Examiner has relied on Paragraph 0009 from Grupe to make a prior art showing of appellant's claimed "queuing additional data to be scanned by the scanning co-processor while waiting for the results from the scanning co-processor" (see this or similar, but not necessarily identical language in the independent Claims 34 and 35).

> "The invention recognises the above problem of scans of computer data that take so long that a complete scan of the data cannot be performed during slack time, such as overnight or during the weekend. To address **this problem embodiments of the invention transfer data to be scanned from a source computer to a scanning computer. The scanning computer then scans the data and creates a log file identifying portions of the data that have predetermined characteristics indicating a particular specified content.** This enables the source computer to rescan or otherwise selectively process the data identified in the log file, which considerably reduces the processing time of the source computer needed for a scan." (Paragraph 0009 - emphasis added)

Appellant respectfully asserts that the excerpt from Grupe relied upon by the Examiner merely discloses that "data to be scanned [is transferred] from a source computer to a scanning computer"

where "[t]he scanning computer **then** scans the data and creates a log file identifying portions of the data that have predetermined characteristics indicating a particular specified content" (emphasis added). However, the mere disclosure in Grupe that the data to be scanned is transferred to the scanning computer where the scanning computer then scans the data and creates a log file fails to even suggest "queuing additional data to be scanned by the scanning co-processor **while** waiting for the results from the scanning co-processor" (emphasis added), as claimed by appellant. Clearly, transferring the data to be scanned and then scanning the data, as in Grupe, fails to suggest "queuing additional data to be scanned... **while** waiting for the results from the scanning co-processor" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 04/27/2007, the Examiner has further relied on Paragraph 0034 of Grupe and has claimed that "Grupe discloses the files are sent and scanned by the scanning computer and once all the files have been scanned the log is sent to the source computer." The Examiner has further stated that "[t]herefore, the files that have yet to be scanned are stored while waiting for the results because the results are not sent until all of the data has been scanned."

Appellant respectfully disagrees with the Examiner's allegations, and asserts that the excerpt from Grupe relied on by the Examiner merely teaches that "all of the files from [a] volume... of the main computer are copied to a scanning computer" and that "[t]he scanning computer then scans the copied files" (Paragraph 0034 – emphasis added). Further, Grupe discloses that "[w]hen all the copied files have been scanned the log file is sent back to the main computer" (Paragraph 0034 – emphasis added). However, merely copying all files to a scanning computer, scanning all copied files, and sending a log back to a main computer after all files have been scanned, as in Grupe, does not teach "queuing additional data to be scanned by the scanning co-processor while waiting for the results from the scanning co-processor" (emphasis added), as claimed by appellant. Clearly, copying the files to a scanning computer, and then scanning the copied files, as in Grupe, simply fails to even suggest that "queuing additional data to be scanned... while waiting for the results" (emphasis added), in the manner as claimed by appellant.

Further, the Examiner has relied on Paragraph 0015 from Grupe to make a prior art showing of appellant's claimed "processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is not

detected" (see this or similar, but not necessarily identical language in the independent Claims 34 and 35).

> "A further aspect of the present invention provides a computer program product comprising a computer program operable to control a source computer to scan computer data stored by said source computer to identify one or more portions of said computer data having one or more predetermined characteristics indicative of said computer data having some specified content, said computer program comprising: **log reading logic operable to control said source computer to read a log file written by a scanning computer, said log file identifying portions of said computer data having said predetermined characteristics; and response logic responsive to said log file and operable to control said source computer to perform further processing tasks upon at least said data identified in said log file as having said predetermined characteristics.**" (Paragraph 0015 - emphasis added)

Appellant respectfully asserts that the excerpt from Grupe relied upon by the Examiner merely discloses that "log reading logic [is] operable to control said source computer to read a log file written by a scanning computer [where] said log file identif[ies] portions of said computer data having said predetermined characteristics" (emphasis added). Further, Grupe discloses that "said source computer ... perform[s] further processing tasks upon at least said data identified in said log file as having said predetermined characteristics" (emphasis added). However, the mere disclosure of performing further processing tasks upon a log file which identifies portions of computer data having predetermined characteristics, as in Grupe, fails to even suggest "processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is **not** detected" (emphasis added), as claimed by appellant.

In the Office Action mailed 05/01/2006, the Examiner has argued that "the log file allows the user to ascertain which data is malicious (needing re-scanning)" and "[t]he other data is clean." Appellant respectfully disagrees and asserts that Grupe merely discloses that "said log file identif[ies] portions of said computer data having said predetermined characteristics" (emphasis added). Clearly, identifying portions of computer data having predetermined characteristics fails to even suggest "the receipt of favorable results from the scanning co-processor including a situation where malicious code is **not** detected" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 04/27/2007, the Examiner has further relied on Paragraphs 0017 and 0030 of Grupe and has argued that "[w]hen the live system receives the log file containing a list of infected files, any file that is not on the list has favorable results." The Examiner has further argued that "[t]herefore when the files copied from the live system to the backup system are the complete set of files stored on the computer (see paragraph [0031]), the files not in the log file would be utilized as normal by the live system."

Appellant respectfully disagrees and notes that the above excerpts from Grupe relied on by the Examiner merely teach that "a copy of the live data on a "live" system… is sent… to a backup system" (Paragraph 0030). The excerpts further teach that "[t]he backup system then scans… the copied data for predetermined characteristics… creates a log file and writes… details of such data to the log file… [and] sends… the log file back to the live system" (Paragraph 0030). Further, the excerpts teach that "[t]he live system then scans any live data that is indicated in the log file" (Paragraph [0030] – emphasis added), where "said log file identif[ies] portions of said computer data having said predetermined characteristics" (Paragraph 0015 – emphasis added).

However, appellant points out that simply nowhere in the above excerpts from Grupe relied on by the Examiner is it taught that "any file that is not on the list has favorable results," as claimed by the Examiner. The above excerpts teach that "said log file identif[ies] portions of said computer data having said predetermined characteristics;" thus, any portions of computer data not on the list simply do not have the predetermined characteristics that the backup system scanned for.

Further, merely scanning copied data for predetermined characteristics, creating and sending a log file, and scanning data indicated in the log file that has the predetermined characteristics fails to even suggest "the receipt of favorable results from the scanning co-processor," much less "processing the data utilizing the central processing unit upon the receipt of favorable results from the scanning co-processor including a situation where malicious code is not detected" (emphasis added), as claimed by appellant. Clearly, a log file containing details of data with predetermined characteristics, as in Grupe, simply fails to suggest "the receipt of favorable results from the scanning co-processor including a situation where malicious code is not detected" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that appellant's specific claim language is not anticipated by the Grupe reference since all of appellant's claim limitations have not been met by the Grupe reference, as noted above.

Group #6: Claim 38

The Examiner has relied on Paragraph 0036 in Grupe to make a prior art showing of appellant's claimed technique "wherein the criteria is further based on a user."

> "In the above embodiments the scanning of files is generally done to detect such things as viruses and worms. However, **embodiments of the above invention can be used to detect any content of a file that the user specifies.** Thus, if a system administrator wishes a particular games program to be banned from the system details of the program can be added to the library of data to be scanned for. Alternatively if a check on all e-mail is required in order to confirm, for example, that there is no pornographic material present, then a scan of the stored volume of mail for particular banned words can be made." (Paragraph 0036 - emphasis added)

Appellant respectfully asserts that the excerpt from Grupe relied upon by the Examiner teaches that "embodiments of the above invention can be used to detect any content of a file that the user specifies" (emphasis added). However, detecting user specified content of a file, as in Grupe, fails to even suggest a technique "wherein the criteria is further based on a user" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 04/27/2007, the Examiner has argued that 'Grupe discloses, "embodiments of the above invention can be used to detect any content of a file that the user specifies"' and that "[t]herefore, the content that the user specifies is the criteria and since the user selected these criteria it is based on the user."

Appellant respectfully disagrees and again points out that the excerpt from Grupe relied on by the Examiner merely teaches that "embodiments of the above invention can be used to detect any content of a file that the user specifies" (emphasis added). In fact, the Examiner admits that "the content that the user specifies is the criteria" (emphasis added). However, detecting user-specified content, as disclosed in Grupe, does not disclose a technique "wherein the criteria is further based on a user" (emphasis added), in the context claimed by appellant (see independent Claim 1 for context).

Again, appellant respectfully asserts that appellant's specific claim language is not anticipated by the Grupe reference since all of appellant's claim limitations have not been met by the Grupe reference, as noted above.

Group #7: Claim 39

The Examiner has relied on Paragraph 0036 in Grupe to make a prior art showing of appellant's claimed technique "wherein the criteria is further based on software logic run by a bios."

> "In the above embodiments the scanning of files is generally done to detect such things as viruses and worms. However, **embodiments of the above invention can be used to detect any content of a file that the user specifies.** Thus, if a system administrator wishes a particular games program to be banned from the system details of the program can be added to the library of data to be scanned for. Alternatively if a check on all e-mail is required in order to confirm, for example, that there is no pornographic material present, then a scan of the stored volume of mail for particular banned words can be made." (Paragraph 0036 - emphasis added)

Appellant respectfully asserts that the excerpt from Grupe relied upon by the Examiner teaches that "embodiments of the above invention can be used to detect any content of a file that the user specifies." However, detecting user specified content of a file, as in Grupe, fails to even suggest a technique "wherein the criteria is further based on software logic **run** by a bios" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 04/27/2007, the Examiner has further relied on Paragraph 0031 of Grupe and has argued that 'Grupe discloses "[t]he files copied from the source computer may be a complete set of files stored on the computer".' Further, the Examiner has alleged that "[t]herefore, when all the files are sent as a criterion for scanning, the software logic that is run by a bios is included with these files and therefore the criteria is based on software logic run by a bios."

Appellant respectfully disagrees with the Examiner's allegations and asserts that nowhere in the excerpts from the Grupe reference relied on by the Examiner is it disclosed that "the software logic that is run by a bios is included with these files and therefore the criteria is based on software logic run by a bios," as alleged by the Examiner. Appellant asserts that the excerpts from Grupe relied

upon by the Examiner merely disclose that "[t]he files copied from the source computer may be a complete set of files stored on the computer" (Paragraph 0031). However, the mere disclosure of copying a complete set of files from the source computer, as in Grupe, fails to teach a technique "wherein the criteria is further based on software logic **run** by a bios" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that appellant's specific claim language is not anticipated by the Grupe reference since all of appellant's claim limitations have not been met by the Grupe reference, as noted above.

Group #8: Claim 44

The Examiner has relied on Paragraph 0016 in Grupe to make a prior art showing of appellant's claimed technique "wherein the central processing unit aids the scanning co-processor when a large amount of data is to be scanned."

> "In some embodiments of the invention said computer data comprises a fraction of data stored on said source computer, **said computer program product being operable to control said source computer to transmit at least one further fraction of said data to at least one further scanning computer, and to control said source computer to receive a log file from each of said at least one further scanning computers.** By dividing the data to be scanned into different fractions and sending each fraction to a different scanning computer, a scan can be performed in less time that it would take a single scanning computer. Thus, in a situation where it was not possible to do a complete scan during a slack period, such as overnight, on a single computer, it may be possible to perform such a scan on a plurality of computers." (Paragraph 0016 - emphasis added)

Appellant respectfully asserts that the excerpt from Grupe relied upon by the Examiner teaches that "said computer program product being operable to control said source computer to transmit at least one further fraction of said data to at least one further scanning computer, and to control said source computer to receive a log file from each of said at least one further scanning computers" (emphasis added). However, the mere disclosure that the source computer transmits one further fraction of said data to at least one further scanning computer, as in Grupe, fails to even suggest a technique "wherein the central processing unit **aids** the scanning co-processor when a large amount of data is to be scanned" (emphasis added), as claimed by appellant. Clearly, transmitting a fraction of data to

several scanning computers, as in Grupe, fails to suggest that the "the central processing unit aids the scanning co-processor" (emphasis added), in the manner as claimed by appellant.

In the Examiner's Answer dated 04/27/2007, the Examiner has argued that '[s]ince the source computer has "a computer program operable... to scan computer data", it is a scanning computer." Further, the Examiner has further argued that "[t]herefore, when the dividing as taught in paragraph [0016] is performed the source computer would also scan a fraction of the data in order to complete the scan during a slack period, such as overnight."

Appellant respectfully disagrees and asserts that nowhere in the Grupe reference is it specifically disclosed that "when the dividing as taught in paragraph [0016] is performed the source computer would also scan a fraction of the data," as asserted by the Examiner. Further, appellant again asserts that the mere disclosure that the source computer transmits a further fraction of data to at least one further scanning computer, as in Grupe, fails to even suggest a technique "wherein the central processing unit **aids** the scanning co-processor when a large amount of data is to be scanned" (emphasis added), in the context claimed by appellant.

Also, appellant respectfully points out that Grupe discloses "dividing the data to be scanned into different fractions and sending each fraction to a different scanning computer" when "in a situation where it was not possible to do a complete scan during a slack period" (Paragraph 0016 – emphasis added). Clearly, dividing the data to be scanned into different fractions and sending each fraction to a different scanning computer, as in Grupe, fails to teach a technique "wherein the central processing unit aids the scanning co-processor when a large amount of data is to be scanned" (emphasis added), in the context claimed by appellant.

Again, appellant respectfully asserts that appellant's specific claim language is not anticipated by the Grupe reference since all of appellant's claim limitations have not been met by the Grupe reference, as noted above.

Issue #3:

The Examiner has rejected Claims 3, 19, 36, 41 and 43 under 35 U.S.C. 103(a) as being unpatentable over Grupe et al. (U.S. Publication No. 2002/0194212), in view of Zuta (International Publication No. WO 98/45778).

Group #1: Claims 3, 19, and 43

Appellant respectfully asserts that such claims have not been met by the prior art by virtue of the arguments made in Issue #2, Group #1 above.

Group #2: Claim 36

Appellant respectfully asserts that such claims have not been met by the prior art by virtue of the arguments made in Issue #2, Group #5 above.

Group #3: Claim 41

The Examiner has relied on page 24, lines 1-3 in Zuta to make a prior art showing of appellant's claimed technique "wherein the scanning control logic is executed automatically when a computer is booted up."

> "At power-up the controller 21 loads known viruses pattern as well as sensitive operations which demand further scrutiny, like interrupts or file operations or I/O. The smart verification is detailed below." (Zuta, Page 24, lines 1-3)

Appellant respectfully asserts that such excerpt merely discloses that at power-up "the controller 21 loads known viruses pattern as well as sensitive operations which demand further scrutiny." Clearly, loading a "known viruses pattern" and "sensitive operations which demand further scrutiny" at power-up, as in Zuta, fail to teach a technique "wherein the scanning control logic is executed automatically when a computer is booted up" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 04/27/2007, the Examiner has further relied on Paragraphs 1 and 2 of Page 24 of Zuta and has argued that "when the system is powered up (i.e. booted up) the controller loads the necessary information to detect viruses" and that "since the monitoring means is

detecting viruses thereafter during normal operation, the scanning logic must also be loaded at power-up." The Examiner has further stated that 'on page 6 Zuta discloses "2. controller means 21 to: initiate the monitoring means at start-up",' and also that "this initiating is the scanning control logic automatically being executed since the monitoring means is hardware." Appellant has interpreted this as referring to Paragraph 5 of Page 16 of Zuta.

Appellant respectfully disagrees and points out the Zuta reference merely discloses that "[a]t power-up the controller… loads known viruses pattern as well as sensitive operations" (emphasis added) and that "[d]uring normal operation thereafter, if a virus is detected then the monitoring means act promptly to stop the applications CPU" but makes no mention that "the scanning logic must also be loaded at power-up" (emphasis added), as asserted by the Examiner. Further, appellant notes that the excerpts from Zuta on Page 16 relied on by the Examiner merely disclose "controller means… to: initiate the monitoring means at start-up," where "monitoring means… evaluate operation of first processor in real time for detecting abnormal operation" (Page 16, Paragraphs 4 and 5 – emphasis added). However, merely initiating monitoring means which evaluate processor operation at startup, as in Zuta, does not even suggest a technique "wherein the scanning control logic is executed automatically when a computer is booted up" (emphasis added), in the context claimed by appellant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the first element of the prima facie case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner argued that it would have been obvious to one of ordinary skill in the art at the time of invention to incorporate the ideas of Zuta with those of Grupe and add the use of a bus between the CPU of the first computer and the scanning co-processor of the second computer because a bus is a commonly used method of

transmitting data between two units. Appellant respectfully disagrees with such statement, especially in view of the vast evidence to the contrary.

In the Examiner's Answer dated 04/27/2007, the Examiner has argued "that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or **in the knowledge generally available to one of ordinary skill in the art.**" The Examiner has further argued that "[s]ince a bus is a commonly used method of transmitting data between two units this is motivation known to one of ordinary skill in the art."

Appellant respectfully disagrees and notes that Grupe "relates to data processing systems in which it is desired to scan a plurality of computer files to identify one or more predetermined characteristics indicative of a computer file having some specified content" (Abstract – emphasis added). Additionally, Grupe teaches that "embodiments of the invention are particularly well suited to scanning for… a computer virus" (Paragraph 0011 – emphasis added). However, Zuta teaches that the "approach to the computer virus" where "the antivirus program scans the memory and compares the patterns therein with… stored patterns" creates a "big problem" since "only known viruses… can be detected" and "antivirus programs cannot prevent damage from new viruses which are not included therein" (Page 3, Paragraphs 3 and 5 – emphasis added). Zuta also teaches that the above approach has "[a]nother problem" since "the memory is only scanned prior to its use" and that "[a] self-changing virus can become active after it was scanned" (Page 4, Paragraph 1 – emphasis added). Thus, Zuta's disclosure that antivirus programs cannot prevent damage from self-changing viruses in fact *teaches away* from using Grupe's method of scanning computer files to identify predetermined characteristics indicative of a computer file having specified content. It is improper to combine references where the references teach away from their combination. *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983).

Appellant respectfully asserts that at least the first and third element of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue #4:

The Examiner has rejected Claim 37 under 35 U.S.C. 103(a) as being unpatentable over Grupe et al. (U.S. Publication No. 2002/0194212), in view of Snavely (Snavely, Allan; Tullsen, Dean. Symbiotic Jobscheduling for a Simultaneous Multithreading Processor. Published in the Proceedings of ASPLOS IX. November 2000).

Group #1: Claim 37

Appellant respectfully asserts that such claims have not been met by the prior art by virtue of the arguments made in Issue #2, Group #5 above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P014).

Respectfully submitted,

By: /KEVINZILKA/ Date: June 26, 2007
Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660